MONTANA CHEMICAL DEPENDENCY CENTER POLICY AND PROCEDURE MANUAL

Policy Subject: Computer Use Protocol	
Policy Number: CUP 01	**Standards/Statutes: 2-17-501, MCA; 2-17-503, MCA; 2-15-114, MCA; 2-17-302 MCA; 45-6-311, MCA; 45-8-213 MCA; ARM2.13.101-2.13.107; Summit Net Acceptable Use Policy; Internet Service Policy; Electronic Mail Policy; Internet/Intranet Security Policy; Federal Electronic Communications Privacy Act; Montana Constitution Article II, 9-10**
Effective Date: 01/01/02	**Page 1 of 8**

PURPOSE:
A guide for properly using and protecting Montana Chemical Dependency Center's Information Technology Resources. And, to provide proper computer protocol and procedures according to State statues and standards in the use of state computers.

POLICY:
Problems or needs related to the computer are to be directed to the Information Systems Technician (IST). If the IST is unable to solve your issue, the appropriate channels will be contacted to assist in resolving the problem.

Information Technology *(IT)* is the employment of computer hardware, software, networks and telecommunications. The Montana Chemical Dependency Center uses IT to conduct business, deliver services and education, communicate with colleagues and patients, and make decisions.

PROCEDURE:
All state policy and procedures will be followed at this facility. The following are some In-house rules that all staff will need to be aware of.
As a state employee, it is your responsibility to safeguard the state's IT investment by following these guidelines:
Use state property for state (appropriate) purposes.
Protect state property; keep it safe and secure.
Use state property within the limits of that property.
Protect the state from liability resulting from the misuse of the property; use property legally. State

information technology property includes not only the computers your work on, but also the software you use, the data you create, and the network it is connected to.

It is the responsibility of the Administrator to promote the importance of security matters by ensuring that all employees are provided with security commensurate with their responsibilities. The IST will offer regular classes on Security.

LAWS AND RULES

It is a federal crime to use or distribute unlicensed copies of copyrighted software. Federal laws relating to copyrights, patents, and interstate theft apply to the information technology arena. Generally, copyright laws apply to software; patent laws apply to hardware; and laws on theft apply to hardware, software and data.

USE OF EQUIPMENT

Section 2-2-121 MCA (Montana Code Annotated). A public officer or a public employee may not use public time, facilities, equipment, supplies, personnel, or funds for the officer's or employees private business purposes...

MONTANA OPERATIONS MANUAL

The MOM does not include legal issues in it automated information systems section. The MOM does provide guidance, for the agency Administrator, regarding system design controls; system documentation, protecting software rights, system security, including requiring system-security training for employees; and home access.

Theft and Destruction

Improper or inappropriate use of IT resources may constitute theft or cause damage to the state's property or public image. Violators will be dealt with in accordance with the agency's discipline handling policy.

Unauthorized Mainframe Access. All unauthorized-access attempts against protected data on the state's mainframe will cause a violation. Agency security officers are provided a daily report showing activity against protected data on the mainframe. This report shows either login information about data activity or violation information for access attempts made to protect resources. The security officer reviews these reports. Violators are contacted if necessary.

Montana Chemical Dependency Center's Information Systems Technician also reviews this report to provide a level of checks and balances. When a user receives a message indicating a violation, he or she should contact the agency security officer to have the problem resolved.

Unauthorized Network and PC (Personal Computer) Access. Unauthorized The Information Systems will monitor attempts to access network data Technician and network security officers. Specific networks may have Policies outlining how violations will be enforced.

Computer Use. Section 45-6-311 MCA. As used in Section 45-6-311 MCA, the term "obtain the use of" means to instruct, communicate with, and store date in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network or to cause another to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network.

Unlawful Use of a Computer. Section 45-6-311 MCA.

A person commits the offense of unlawful use of a computer if the person knowingly or purposely: obtains the use of any computer, computer system, or computer network without consent of the owner; alters or destroys, or causes another to alter or destroy, a computer program or computer software without consent of the owner; or obtains the use of or alters or destroys a computer, computer system, computer network, or any part thereof as part of a deception for the purpose of obtaining money, property, or computer services from the owner of the computer, computer system, computer network, or pa thereof or from any other person. A person convicted of the offense of unlawful use of a computer involving property not exceeding $500 in value shall be fined not to exceed $500, or be imprisoned in the county jail for a term not to exceed 6 months, or both. A person convicted of the offense of unlawful use of a computer involving property exceeding $500 in value shall be fined not more than 2.5 times the value of the property used, altered, destroyed, or obtained; or be imprisoned in the state prison for a term not to exceed 10 years; or both.

Care of IT Equipment

IT equipment includes hardware items such as CPUs (central processing units), monitors, keyboards, modems and other telecommunications devices. These all need proper care and attention.

Keyboards are especially vulnerable to short-circuiting when coffee, pop or other liquids are spilled on them.

Care should be taken that the equipment is not exposed to high temperatures or great temperature fluctuations. UPS (uninterruptible power supplies) and/or surge protectors should be used on computers and printers to spikes and other damaging electrical surges. Printers especially laser printers) should be put on separate UPS or surge protectors. Heaters, coffee pots and other electrical equipment should also be on a separate surge protector or outlet. Turn PCs off during lightning storms, power plant switching or winter line breaks. Do not turn them on again until the building electricity is operating steadily.
Only anti-static cleaners should be used on monitors. Never spray chemicals directly on them.

Security. When stored in a vehicle, all equipment should be kept out of sight. Portable equipment should be in a secured place when not in use.

Location. Adequate ventilation for equipment should be provided, and care should be taken so that the fans and exhaust vents are not obstructed. The network administrator should be contacted before

equipment is moved. When equipment is brought in from a colder environment, it should be give sufficient time to warm up before being used.

Care of Data

Computer data and documents that you create are important. You must be responsible for the accuracy, confidentiality, security and protection of the data. Fortunately, the security and protection of data that is stored on central file servers, departmental computers or the states mainframe computer will be administered by a Information Systems Technician who will be responsible for security and protection (backup) of the data. If your data is stored locally on a PC, it will be your responsibility to secure and backup the data.

Accuracy. Accuracy of information is critical to support the systems with which you will be working and the people for whom you will be working. Take time to double check information entered into a data processing system.

Confidentiality. Confidentiality of information starts with you, so follow policy and common sense with regard to your information. Using any information for gossip or personal gain is never appropriate.

Security. Security of information is your responsibility if not provided by a Information Systems Technician. This means that unauthorized people should not have access to any privileged data with which you work. This responsibility extends to taking reasonable steps to ensure that the information can not be obtained either accidentally or maliciously.

Protection and Backup. Protection of data usually means making a backup, but it actually entails more of a continuous philosophy of making sure that the information can survive disasters, theft, malicious destruction, unauthorized alteration, or most commonly, human mistakes. Backups must be made at intervals determined by the amount and criticality of the information to be protected; stored in a manner such that a single disaster would not destroy all copies of the data; and stored in a way that prevents access by unauthorized personnel. Individuals should be aware of their agency's backup procedures and participate appropriately.

Disaster Recovery. Montana Chemical Dependency Center has a disaster recovery plan. This plan is a formalized set of procedures and actions taken to minimize agency losses due to an interruption in service. Individuals should also be aware of any disaster recovery efforts and support them if requested.

Scanning Software.

Out-going diskettes should also be scanned. This practice can be especially important if a diskette is infected. By knowing the disk was clean when it left your office, the true source of the infection can be more easily tracked. The more hands a diskette passes through before being scanned, the more difficult it becomes to trace the virus source.

Whenever a virus is detected, users must immediately notify their Information Systems Technician, or designated contact person to coordinate virus removal operations. Much of the damage attributed to

viruses occurs through improper removal attempts.

Virus Hoaxes. A virus hoax is an e-mail message warning users of a new virus being passed around. The first warning sign of a hoax is if it has been forwarded or sent to a list of people. Another sign to look for is the way the message is written. Every e-mail hoax exists to replicate itself as many times as possible, and therefore, will include two things: it will instigate an emotional response and then urge readers to act of their emotions by forwarding the message to a group of people or as many people as possible. Employees should forward these types of messages to their agency security officer or the state security officer and then delete them. They should not be forwarded to groups of people without checking for their authenticity.

Software Licensing

The following definitions are from Prentice Hall's Illustrated Dictionary of Computing.

Software Definitions

Freeware. Utilities and software programs (under copyright) made available to the public free of charge.

Shareware. Software, which is protected under copyright and made available to users on a trial basis, on the condition that if the program is adopted, the user will forward payment to the author. Shareware is often distributed via mail order or copied from public bulletin boards. This differs from public domain software, which is available for use free of charge because it is not protected under copyright.

Software. A computer program; a set of instructions written in a specific language that commands the computer to perform various operations on data contained in the program or supplied by the user.

License Definitions

License Agreement. The agreement that accompanies computer software. Read it! It may be stated explicitly in the software documentation or on the computer screen when the program is opened or implicitly, in the purchase price of the software. In most countries, the legal purchase of software licenses the software user to make one backup copy only, in case the original software disk malfunctions or is destroyed.

Site License. A license from a software publisher which permits an organization to make a large number (limited) of copies of the software in order to equip all network users with personal or shared copies of the program. This is generally far cheaper than purchasing multiple copies of the package. License terms can be perpetual or restricted to a number of months or years.

Network Licensing. On many networks, there is not a one-to-one relationship between the number of users and the number of software licenses for a certain product. This is because some network licenses require only that licenses be purchased for the number of concurrent users. For example, a state agency with a network of 30 PCs may only need to purchase 10 licenses if the application is not heavily used. Anyone in the agency can use the application, but only 10 people at a time will be allowed access.

Work/Home Licensing. Each software publisher has unique guidelines and requirements for their own products. Home use depends on the specific license terms and conditions of the software. In the case of network software, contact your network administrator. The Information Systems Technician can research the license of the software you are interested in using at home and make you aware of the parameters.

NOTE: The Microsoft Office license negotiated by the State does not allow a workplace license to be used at home even if the use is not concurrent. An additional license for the home PC must be purchased.

Copyright Laws

Software Piracy. The criminal act of making or distributing for financial gain, an unauthorized copy (or copies) of a copyrighted software product.

It is illegal to: Copy or distribute software or its accompanying documentation, including programs, applications, data, codes, and manuals, without permission or license from the copyright owner; and run purchased, copyrighted software on two or more computers simultaneously unless the license agreement specifically allows it.

Current Standards

Software. There are specific state standards for microcomputer soft and for supported mainframe software

State Software Standards
Word Processing Microsoft Word
Spreadsheets Microsoft Excel

Electronic Mail (E-mail) Microsoft Exchange/Outlook
Operating System Windows 95
Network Operating System Novellas NetWare
Patient/Server Database Oracle
End-User Database Microsoft Access
Virus Scanning Software Network Associates (McAfee) Virus Scan

Hardware. The state has also established term contracts for personal computers. Currently, agencies have a choice of equipment provided by IBM and Dell. This hardware is guaranteed to be compatible with the states network environment, thereby easing installation and support requirements.

User Responsibilities
Each user on the Montana Chemical Centers computer system is responsible for having knowledge of the Montana Chemical Centers policies concerning their computer. It is the responsibility of the State to educate its management and staff about these policies and to educate it employees about the dangers of computer abuse and its threat to the operation of the State computer network. The State is also responsible for educating its management and staff about proper ethical behavior, acceptable computing practices, and copyright and licensing issues.

Each user of the Montana Chemical Center's computing and information resource must act responsibly. All users of State-owned or State-leased computing systems must be knowledgeable of and adhere to agency policies. They must also respect the rights of other users by minimizing unnecessary network traffic that might interfere with the ability of other employees to make effective use of the shared network resources. Users must respect the integrity of the physical facilities and controls, and obey all federal, state, county, and local laws and ordinances.

Electronic Mail

The State provided electronic mail (e-mail) system is to be used for: the conduct of state and local government business and delivery of government services; transmitting and sharing of information among governmental, research, and educational organizations; communicating and exchanging professional information; and conducting other appropriate State business. Appropriate State business may include office related functions or announcements.

Privacy of e-mail is not guaranteed. Employees should not have expectations of privacy for any messages. Information Systems Technician, management, and Department of Administration personnel can monitor e-mail for performance, troubleshooting purposes, or if abuses are suspected.
Employees should use their best judgment in sending confidential messages of the e-mail system. The use of encryption should be considered when sending these types of messages.

Statewide distributions of mail are not allowed. The Information Systems Technician should be contacted for correct procedures for large distribution.
The use of derogatory, racially offensive, sexually offensive, harassing, or discriminatory communications or conduct will not be tolerated. Misuse of e-mail can result in disciplinary action appropriate to the misuse, up to and including terminations, as administered under policy 3-0130,

Discipline Handling, Montana Operations Manual.

Circulating chain letters is not permitted. Unsolicited mail, or spam, should be deleted immediately. If delivery of spam persists, the Information Systems Technician should be contacted. Employees should not reply to any unsolicited e-mail.

Internet Services

The State provided Internet services are to be used for: the conduct of state and local government business and delivery of government services; transmitting and sharing of information among governmental, research, and educational organizations; supporting open research and education in and between national and international research and instructional institutions; communicating and exchanging professional information; encouraging debate of issues in a specific field of expertise; applying for or administering grants or contracts; announcing requests for proposals and bids; announcing new services for use in research or instruction; conducting other appropriate State business.

Each agency must have a clear policy on their business use of the Internet. The policy should detail the

permissible and non-permissible uses of the Internet for their agency business use. Employees should check with their agency policy person to find out what the agency policy is regarding the Internet.

Revisions:

Prepared By: Rona McOmber Information System Technician 09/26/01
Name Title Date

Approved By: _____ 01/01/02
David J. Peshek, Administrator